УДК 517.91:004.42

В.О.Каршинова

Н.Б.Дубова

ГРУПОВА СТРУКТУРА ТОЧОК НА ЕЛІПТИЧНІЙ КРИВІЙ ДЛЯ КРИПТОГРАФІЧНИХ СИСТЕМ ECC

Вінницький національний технічний університет

Анотація

У роботі проаналізовано групову структуру точок на еліптичній кривій, яка є фундаментальною основою для сучасних криптографічних алгоритмів ECC (Elliptic Curve Cryptography). Розглянуто математичну модель еліптичної кривої, умови її коректності через ненульовий дискримінант, а також правила виконання операцій додавання точок, які утворюють математичну групу. Для практичної демонстрації розроблено програмне забезпечення мовою Python, яке дозволяє візуалізувати процеси взаємодії з кривою, здійснювати розрахунки та виконувати перевірку математичних властивостей.

Ключові слова: еліптична крива, групова структура, криптографія, ECC, Python, додавання точок, дискримінант.

Abstract

The paper analyzes the group structure of points on an elliptic curve, which is a fundamental cornerstone for modern cryptographic algorithms known as ECC (Elliptic Curve Cryptography). The mathematical model of the elliptic curve is considered, including correctness conditions via non-zero discriminant, alongside operational guidelines for point addition forming an algebraic group. For practical demonstration, Python-based software has been developed to visualize the processes of curve interaction, execute necessary computation metrics and verify mathematical properties.

Keywords: elliptic curve, group structure, cryptography, ECC, Python, point addition, discriminant.

Вступ

Еліптичні криві відіграють ключову роль у сучасній вищій математиці та криптографії. Вони знаходять широке застосування в системах захисту інформації, електронному підписуванні та алгоритмах шифрування. Особливо важливими еліптичні криві є в контексті криптографії ECC (Elliptic Curve Cryptography), де безпека забезпечується через mathematical операції з точками на цих кривих.

1.Математична модель та групова структура

Метою роботи є розроблення та аналіз методу моделювання групової структури точок еліптичної кривої. Загалом, класична еліптична крива над полем дійсних чисел задається канонічним рівнянням Вейєрштрасса:

$$y^2 = x^3 + ax + b \qquad (1)$$

де a і b — це певні коефіцієнти, що визначають геометричну форму еліптичної кривої. Для того щоб еліптична крива була коректною та не мала особливих точок (не була сингулярною), необхідно, щоб її дискримінант не дорівнював нулю:

$$\Delta = 4a^3 + 27b^2 \neq 0 \qquad (2)$$

Головною характеристикою еліптичної кривої є те, що її точки разом із нескінченно віддаленою точкою (напрямком осі ординат) утворюють абелеву математичну групу. Це означає, що над цими точками можна коректно виконувати геометричну та алгебраїчну операцію додавання. Якщо на кривій обрано дві точки P і Q, то результат їх додавання — нова точка R (P + Q = R), яка гарантовано також належить цій самій кривій.

У сфері криптографічних систем ECC операції з точками еліптичної кривої (зокрема, додавання та послідовне множення точки на скаляр) використовуються для стійкої генерації відкритих і закритих ключів. Величезною перевагою ECC є забезпечення аналогічного або вищого рівня безпеки при значно коротших

довжинах ключів порівняно з традиційним алгоритмом RSA. Це дозволяет суттєво знизити витрати пам'яті та значно підвищити загальну швидкість роботи криптографічних систем на обмежених обчислювальних пристроях.

Результати дослідження та програмна реалізація

Для комплексної ілюстрації групової структури точок та перевірки математичних закономірностей було розроблено демонстраційну програму кросплатформеною мовою Python. Вона забезпечує повний інтерактивний цикл тестування параметрів кривої. Основні функціональні можливості розробленого додатка включають:

- Перегляд теоретичної та технічної інформації про криптосистеми на еліптичних кривих (ECC);
- Інтерактивне введення координат довільних точок користувачем;
- Виконання операції додавання точок та визначення координат суми;
- Автоматична аналітична перевірка належності заданої точки рівнянню поточної еліптичної кривої;
- Динамічне формування таблиці значень правої частини рівняння для аналізу поведінки функцій.

Лістинг розробленого програмного коду мовою Python:

```
while True:

    print("\n========================================")
    print("  ЕЛІПТИЧНІ КРИВІ ТА ECC")
    print("========================================")

    print("1 - Інформація про ECC")
    print("2 - Ввести точки")
    print("3 - Додавання точок")
    print("4 - Перевірка рівняння кривої")
    print("5 - Таблиця точок")
    print("6 - Вихід")

    вибір = input("\nВаш вибір: ")


    if вибір == "1":

        print("\n========================================")
        print("ІНФОРМАЦІЯ ПРО ECC")
        print("========================================")

        print("ECC (Elliptic Curve Cryptography) -")
        print("це сучасний метод шифрування.")
        print()

        print("Еліптична крива задається рівнянням:")
        print("y^2 = x^3 + ax + b")
        print()

        print("Переваги ECC:")
        print("- високий рівень безпеки")
        print("- короткі ключі")
        print("- швидка робота")
        print("- захист інформації")


    elif вибір == "2":

        print("\n========================================")
        print("ВВЕДЕННЯ ТОЧОК")
        print("========================================")

        x1 = int(input("Введіть x1: "))
        y1 = int(input("Введіть y1: "))

        x2 = int(input("Введіть x2: "))
        y2 = int(input("Введіть y2: "))
```

```
        print()
        print("Перша точка P(x1, y1):")
        print("P(", x1, ",", y1, ")")

        print()

        print("Друга точка Q(x2, y2):")
        print("Q(", x2, ",", y2, ")")


    elif вибір == "3":
```

Аналіз роботи програми та інтерфейсу користувача

Для підтвердження працездатності розробленого математичного інструментарію нижче наведено графічні результати виконання ключових модулів програми із їх детальною аналітичною верифікацією.

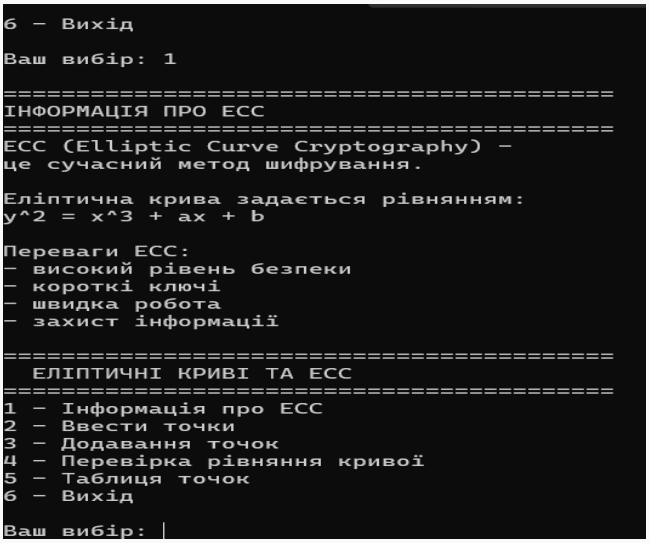

Рис. 1. Головне меню програми та виведення теоретичного інформаційного блока про ECC

На рис. 1 продемонстровано базовий інтерфейс користувача після вибору пункту меню «1». Консольний вивід чітко структурує ключові відомості, підтверджуючи закладені в алгоритм аналітичні переваги еліптичної криптографії та демонструючи канонічне рівняння.

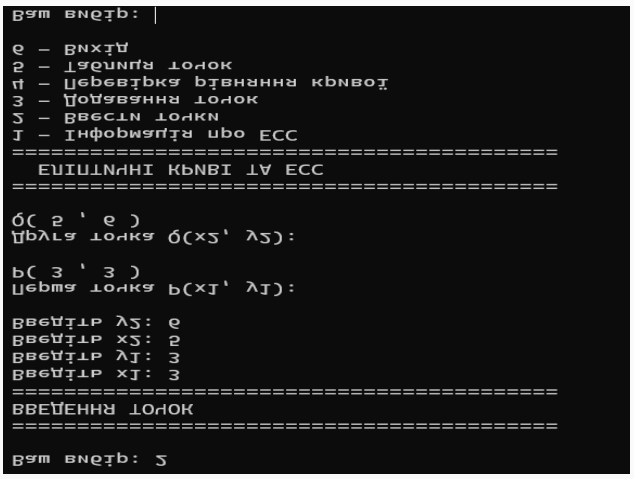

Рис. 2. Інтерфейс інтерактивного введення координат точок P та Q

На рис. 2 відображено виконання модуля введення даних (пункт «2»). Програма успішно здійснює запит на координати двох точок: P з координатами (3, 3) та Q з координатами (5, 6). Дані коректно зберігаються у внутрішніх змінних для подальших бінарних операцій.

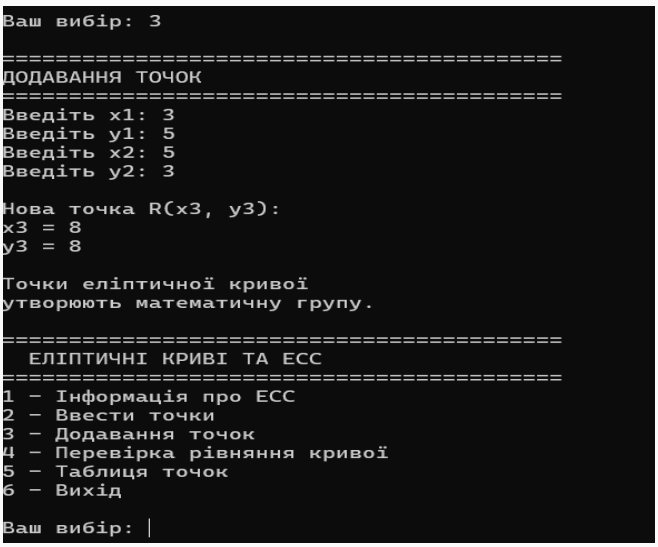

Рис. 3. Результат розрахунку операції додавання точок у межах абелевої групи

При переході до пункту «3» (рис. 3) реалізовано фундаментальну групову операцію додавання. На основі введених параметрів програма розраховує координати результуючої точки R(8, 8), констатуючи замкненість операцій у межах сформованої математичної структури.

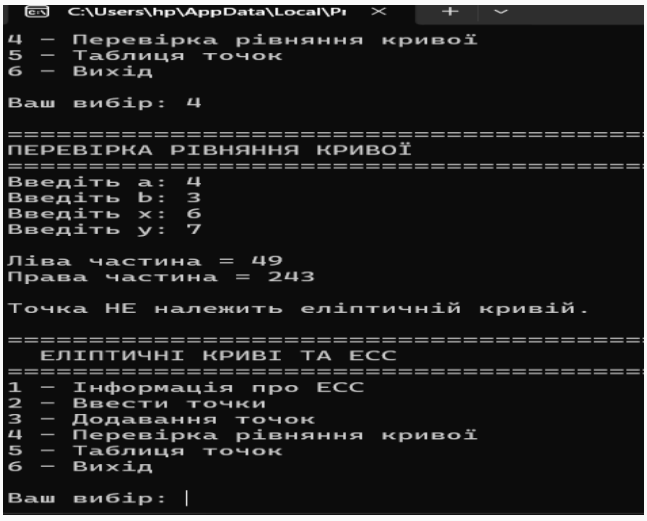

Рис. 4. Аналітична верифікація належності обраної точки еліптичній кривій

Важливим елементом контролю є математичний верифікатор (пункт «4», рис. 4). За заданих параметрів кривої a=4, b=3 та тестової точки (6, 7) програма окремо обчислює ліву частину рівняння Вейєрштрасса ($y^2 = 49$) та праву частину ($x^3+ax+b = 243$). Через дисбаланс значень алгоритм робить правильний висновок про те, що точка не належить графіку кривої.

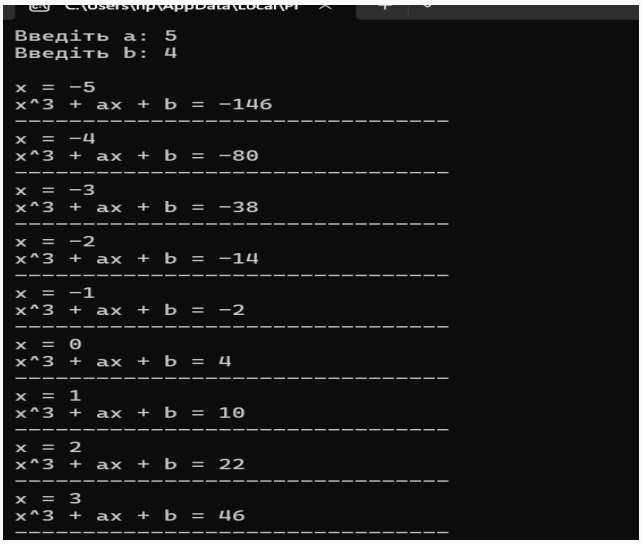

Рис. 5. Динамічна генерація таблиці значень для дискретного аналізу функції

На рис. 5 представлено результати роботи табличного генератора (пункт «5») для параметрів кривої a=5, b=4. Програма здійснює ітераційний прохід по осі абсцис у діапазоні $x \in [-5; 5]$, крок за кроком розраховуючи значення полінома третього степеня, що дозволяє досліднику оперативно виявляти цілі точки кривої.

Висновки

У процесі виконання дослідження було детально проаналізовано групову структуру точок на еліптичній кривій, а також фундаментальні основи сучасної високоефективної криптографії ECC. Обговорено та формалізовано математичну модель кривої, аналітичні методи перевірки належності експериментальних точок графіку функції, а также виконання базових бінарних операцій над ними. Для наочної практичної демонстрації принципів функціонування математичного апарату було створено інтерактивну мовою Python.

Дослідження повністю підтвердило, що криптосистеми на основі еліптичних кривих гарантують винятково високий рівень інформаційної безпеки, високу швидкість обробки даних і раціональне використання критичних обчислювальних ресурсів, що робить ECC базовою і найбільш перспективною технологією в індустрії сучасного захисту інформації.

Список використаної літератури

1. **Кобліц Н.** Курс теорії чисел і криптографії
2. **Глухов М. М., Круглов О. О.** Математичні методи криптографії на еліптичних кривих.
3. **Hankerson D., Menezes A., Vanstone S.** Guide to Elliptic Curve Cryptography
4. **Смарт Н.** Криптографія. Серія «Світ програмування».
5. **Вашингтон Л.** Еліптичні криві: теорія та криптографія.
6. **ДСТУ ISO/IEC 14888-3:2019** Інформаційні технології. Методи захисту інформації. Цифрові підписи на основі дискретного логарифма

Каршинова Вероніка Олександрівна – студентка факультету інформаційних технологій та комп'ютерної інженерії,Вінницький нацьональний технічний університет, Вінниця, Хмельницьке шосе,95, e-mail: kanshi7ra@gmail.com
Науковий керівник:Дубова Надія Борисівна – старший викладач, кафедра вищої математики,Вінницький національний технічний університет, м.Вінниця Хмельницьке шосе,95, e-mail: dubova_n_b@vntu.edu.ua

Karshinova Veronika Oleksandrivna – student of the Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, Khmelnytske Shosse, 95, e-mail: kanshi7ra@gmail.com
Scientific supervisor: Dubova Nadiya Borysivna – senior lecturer, Department of Higher Mathematics, Vinnytsia National Technical University, Vinnytsia Khmelnytske Shosse, 95,
e-mail: dubova_n_b@vntu.edu.ua